ベクトル空間アクセス構造を用いた秘密分散法 (代数と言語のアルゴリズムと計算理論)

AUTHOR(S):

足立, 智子; 藤井, 聖子

CITATION:

足立, 智子 ...[et al]. ベクトル空間アクセス構造を用いた秘密分散法 (代数と言語のアルゴリズムと計算理論). 数理解析研究所講究録 2011, 1769: 169-179

ISSUE DATE:

2011-10

URL:

http://hdl.handle.net/2433/171468

数理解析研究所講究録
第1769巻 2011年 169-179

ベクトル空間アクセス構造を用いた秘密分散法

東邦大学　理学部　情報科学科
足立　智子，藤井　聖子
Toho University, Department of Information Science
Tomoko Adachi, Seiko Fujii

要旨　秘密情報を復元できる権限を持つ参加者部分集合の族をアクセス構造という。本稿では、ベクトル空間アクセス構造を紹介する。さらに、会合数1の場合に、グラフを用いたアクセス構造との対応についても述べる。

1. はじめに

秘密情報をn人に分散し、任意のt人の合意があれば秘密情報が復元できるが、t人未満では復元できない。これがShamirの(t,n)しきい値法[3]と呼ばれる秘密分散法である。秘密分散法の考え方は、核兵器制御スイッチ(秘密情報)の制御方法にも採り入れられている。Time Magazine (1992)によれば、ロシアでは大統領・国防大臣・国防省の三人のうち二人が合意すれば、核爆弾投下が決行できる仕組みになっている。現在では、クラウドコンピューティングでも採り入れられており、NRIセキュアテクノロジーズは2010年10月より秘密分散技術を用いて分割した重要データを複数のデータセンターで管理するサービスを提供している。

秘密情報の復元に必要な参加者を、任意のt人ではなく、決められた参加者の部分集合としたい場合には、アクセス構造を用いる。先の例を用いると、どの2人からも秘密情報が復元できるのではなく、大統領を含めた2人でないと秘密情報が復元できないような場合である。1989年、Brickellによってベクトル空間を用いたアクセス構造[1]が提案された。本稿では、ベクトル空間アクセス構造を持つ秘密分散法における分散情報の配布や秘密情報の復元の方法を紹介する。さらに、会合数が1である場合について、グラフを用いたアクセス構造との対応[2]についても紹介する。

2. ベクトル空間アクセス構造

秘密分散法を実現する代表的な方法として、Shamirの(t,n)しきい値法がある。これは、n人の参加者集合Πのうち、任意のt人が持つ分散情報yから秘密情報

Sが復元できる方法である。より一般的な方法として、秘密情報Sを復元できる参加者集合と復元できない参加者集合に分類するアクセス構造がある。本節では、アクセス構造による秘密分散法をベクトル空間上で構成するBrikellの方法を紹介する。

2.1 アクセス構造

参加者集合のうち，秘密情報を復号できる権限を持つ集合をアクセス集合という。アクセス集合の族をアクセス構造 Γ といい、アクセス集合のうち、一人でも参加者が欠けると秘密情報を復元できなくなる最小の集合を最小アクセス集合といい、この族を最小アクセス構造 Γ_0 という。Γ_0 の要素(最小アクセス集合)を基とも呼ぶ。アクセス構造、および最小アクセス集合を数学的に定義すると以下となる。

定義 2.1　アクセス構造 Γ と最小アクセス構造 Γ_0

参加者集合をΠ、参加者部分集合をB, B'とする。このときアクセス構造 Γ および最小アクセス構造 Γ_0 を以下で定義する。

$$\Gamma := \{B' \subseteq P : B \subseteq B', B \in \Gamma_0\}$$

$$\Gamma_0 := \{B \in \Gamma : B' \setminus \{V_i\} \notin \Gamma \mid V_i \in B',\ i = 1, \cdots, n\}$$

秘密情報の値の情報が非アクセス集合の任意の参加者からは得られないならば完全な秘密分散法といい、本稿においてはこの場合についてのみ考える。

定義 2.2　アクセス構造を実現する完全な秘密分散法

n人の利用者集合Πの中で秘密情報Sを分散させるとき、以下の性質を同時に満たすものを完全な秘密分散法という。

1. アクセス集合$B \subseteq P$の持つ分散情報から秘密情報Sの値を特定できる。
2. 非アクセス集合$N \subseteq P$の持つ分散情報から秘密情報Sの値に関して何も得られない。

2.2 ベクトル空間アクセス構造の構成法

素数をpとし、2以上の整数をdとする。このとき、剰余環$Z_p = \{0,1,2,\cdots,p-1\}$は、位数pの体になる。$Z_p$上のd次元ベクトル空間を$(Z_p)^d$と表し、本稿では、このベクトル空間を用いる。

アクセス構造をΓとする。参加者集合$P = \{P_i \mid 1 \le i \le n\}$と、$\Pi$に属さないディ

ーラーDが存在する。条件

$$\phi(D)=(1,0,\cdots,0)\in\langle\phi(P_i):P_i\in B\subset\Pi,\ i=1,\cdots,n\rangle \ \Leftrightarrow\ B\in\Gamma$$

を満たす写像$\phi:P\cup\{D\}\rightarrow(Z_p)^d\setminus\{0\}$により、参加者それぞれに非零ベクトルを公開値として与える。すなわち、ディーラーDのベクトル$\phi(D)=(1,0,\cdots,0)$は、Bが権限を持つ部分集合であるそのときのみ、集合$\{\phi(P_j):P_j\in B\}$のベクトルの線形結合として表せる。ここで、ベクトル$v_1,v_2,\cdots,v_n$の線型結合$\langle v_i\rangle$とは、ベクトル$v_1,v_2,\cdots,v_n$とスカラー$a_1,a_2,\cdots,a_n$を用い、$a_1v_1+a_2v_2+\cdots+a_nv_n$の形で表されることを意味する。

次に、Brikell法による秘密情報の分散配布、および復元について紹介する。ディーラーDは、秘密情報Sから分散情報V_iを作成し、n人の参加者P_iへ配布する。すなわち、参加者P_iは、公開されているベクトル$\phi(P_i)$と非公開の値である分散情報V_iを所持する。秘密情報Sの復元は、アクセス集合$B\in\Gamma$に含まれる全参加者が集まった時に可能となる。

アルゴリズム2.1　Brikellによるベクトル空間上でのアクセス構造の構成法

Step 1.[初期設定]　pを素数、dを2以上の整数、$1\le i\le n$とする。ディーラーDは$(1,0,\cdots,0)$を除く$(Z_p)^d$から、ベクトル$\phi(P_i)$を選択する。ディーラーDは、ベクトル$\phi(P_i)$を参加者P_iに公開値として与え、秘密情報$S\in Z_p$を保持する。また、Z_p上のd−1個のランダムな要素$r_2,\cdots,r_d$を選択し、ベクトル$\vec{r}=(S,r_2,\cdots,r_d)$を与える。

Step 2.[分散配布]　ディーラーDは分散情報$V_i=\vec{r}\cdot\phi(P_i)$を計算し、参加者$P_i$に非公開に付与する。

Step 3.[復元]　参加者$P_i\in B$が、それぞれベクトル$\phi(P_i)$と分散情報V_iを持ちより$(1,0,\cdots,0)=\sum_{\{i:P_i\in B\}}C_i\,\phi(P_i)$に代入し、この方程式を満たす$C_i$を求める。さらに、参加者$P_i$は、求めた値$C_i$と分散情報$V_i$を持ちより、$S=\sum_{\{i:P_i\in B\}}C_iV_i$により秘密情報Sを復元できる。

次に、p=3, d=4として例を示す。ディーラーDと4人からなる参加者集合$P=\{P_i\mid 1\le i\le 4\}\cdot D$が存在する。ベクトル空間$(Z_3)^2$上でアクセス構造を構成する。今、ディーラーDにはベクトル$\phi(D)=(1,0)$を、4人の参加者P_1, P_2, P_3, P_4各々にはベクトル$\phi(P_1)=(1,1)$, $\phi(P_2)=(2,1)$, $\phi(P_3)=(1,2)$, $\phi(P_4)=(2,2)$を与える。このとき、$B_1=\{P_1,P_2\}$, $B_2=\{P_1,P_3\}$, $B_3=\{P_2,P_4\}$, $B_4=\{P_3,P_4\}$を基とする最小アク

セス構造$\Gamma_0=\{B_1,B_2,B_3,B_4\}$を考える。図2.1では、4本の太線が4つの基に対応する。

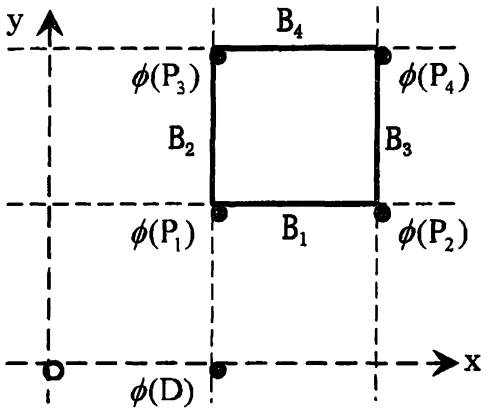


図2.1　ベクトル空間$(Z_3)^2$上における
4人の参加者によるアクセス構造の例

例2.1　ベクトル空間$(Z_3)^2$上でのアクセス構造の構成例

Step 1.[初期設定]　ディーラーDは、ベクトル$\phi(P_1)=(1,1)$，$\phi(P_2)=(2,1)$，$\phi(P_3)=(1,2)$，$\phi(P_4)=(2,2)$を参加者P_iに公開値として与え、秘密情報$S=2\in Z_3$を保持する。また、Z_3上の1個のランダムな要素

$r_2=2$を選択し、$\vec{r}=(2,2)$を得る。

Step 2.[分散配布]　ディーラーDは分散情報$V_i=(2,2)\cdot\phi(P_i)$を計算し、V_iを参加者P_iに非公開に付与する。

$V_1=(2,2)\cdot(1,1)$

同様に、$V_2=0, V_3=0, V_4=2$

Step 3.[復元]　アクセス集合B_1とし、次式を満たすC_iを求める。

$C_1\phi(P_1)+C_3\phi(P_3)=V_1+V_3\quad(1+1)$

連立方程式$\begin{cases}C_1+C_2=1\\C_1+2C_2=0\end{cases}$ mod 3を解き、$C_1=2,C_2=2$を得る。

参加者$P_i\in B$は、求めた値C_iと分散情報V_iを持ち寄り、次式を用いて秘密情報Sを復元できる。

$S=\Sigma C_i\phi(P_i)=C_1V_1+C_3V_3$

3. 会合数1のアクセス構造

はじめに、アクセス構造の連結という概念について紹介する。Γ を参加者集合Π上のアクセス構造とする。任意の参加者$p,q\in P$に対し、$1\le i\le \ell-1$に関して$p\in A_1$, $q\in A_\ell$, $A_i\cap A_{i+1}\neq\varnothing$であるような最小アクセス集合$A_1,\cdots,A_\ell\in\Gamma_0$が存在するなら、アクセス構造 Γ は連結されているという。

グラフ G は、頂点集合$V(G)$と辺集合$E(G)$から成る。このとき、グラフを用いたアクセス構造Γでは、頂点集合$V(G)$が参加者集合Πに対応し、辺集合$E(G)$が最小アクセス構造 Γ_0に対応し、辺が基に対応する。また、基(最小アクセス集合)の参加者の最大人数および最小人数を、それぞれランクおよびコランクといい、rank(Γ), corank(Γ)と表す。

アクセス構造 Γ の会合数とは、2 つの異なる最小アクセス集合に共通する要素(参加者)の最大数のことである。グラフによって定義される会合数 1 のアクセス構造について、2006 年に Jaume Marti-Farre と Carles Padro によって評価がなされた[2]。例 2.1 のベクトル空間$(Z_3)^2$上でのアクセス構造は、グラフによって定義される会合数 1 のアクセス構造である。

以上を踏まえ、本節では、グラフによって定義される会合数 1 のベクトル空間アクセス構造をいくつか紹介する。

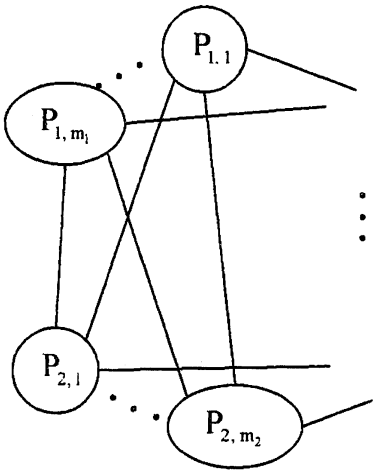


図3.1　完全多部グラフに関するアクセス構造

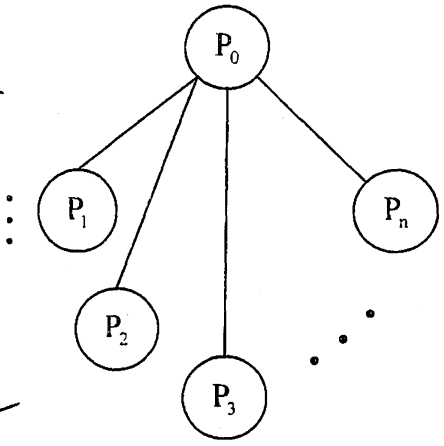


図3.2　星アクセス構造

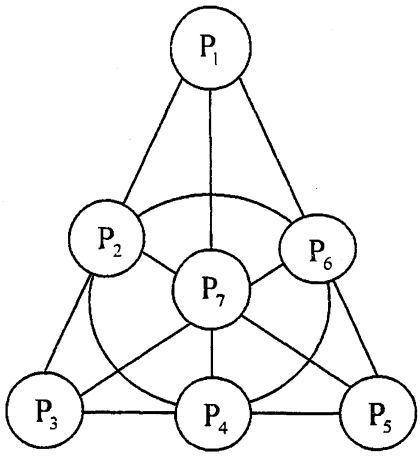


図3.3　ファノ平面に関するアクセス構造

3.1 完全多部グラフに関するアクセス構造

グラフ G の頂点集合$V(G)$を k 個の部分集合$M_j\ (1\le j\le k)$に分割し、これを部分と呼ぶ。このとき$|M_j|=m_j$とする。このとき、任意の辺の両端点が異なる部

分に属しているようなグラフを k 部グラフという。特に、各頂点が自分の属していない部分に含まれる頂点全てと辺で連結しているものを完全多部グラフといい、$K_{m_1,\cdots,m_k}$ で表す。完全多部グラフに関するアクセス構造$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$において、2 つの異なる最小アクセス集合に共通する頂点の最大数は 1 であるので、会合数は 1 である(図 3.1 参照)。

補題 3.1

完全多部グラフに関するアクセス構造$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$は、ベクトル空間アクセス構造である。

証明 3.1

$m_1,\cdots,m_k$ をグラフ G の頂点集合 V(G) の部分 M_j $(1\le j\le k)$ の位数とする。

いま p を素数とし、剰余環 Z_p 上の 2 次元ベクトル空間 $(Z_p)^2$ を考える。Z_p 上の異なる要素を x_i $(1\le i\le n)$ とする。また、それぞれ頂点、すなわち参加者 P_i に与えるベクトルを $\phi(P_i)=(x_i,1)$ とする。つまり、同じ部分に含まれる参加者には同じベクトルを与える。このとき、

$$\phi(D)=(1,0)\in\langle\phi(P_i):P_i\in B\subset\Pi,\ i=1,\cdots,n\rangle \Leftrightarrow B\in\Gamma$$

を確かめるのは容易である。同様に、位数 p の d 次元ベクトル空間において適当なベクトルを与えるときについても確かめることができる。ゆえに、完全多部グラフに関するアクセス構造$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$はベクトル空間アクセス構造である。 □

3.2 星グラフに関するアクセス構造

参加者が 1 人の部分 $\{P_0\}$ と n 人の部分 $\{P_1,\cdots,P_n\}$ から成る完全二部グラフ $K_{1,n}$ を、星グラフ $S(P_0)$ という。この星グラフは、2 つの異なる最小アクセス集合 $A,A'\in\Gamma_0$ に関して、$A\cap A'=\{P_0\}$ であるような $P_0\in P$ が存在するアクセス構造とみなすことができる。このアクセス構造を星アクセス構造$\Gamma\langle S(P_0)\rangle$といい、会合数は 1 である(図 3.2 参照)。

補題 3.2

星グラフに関するアクセス構造$\Gamma\langle S(P_0)\rangle$は、ベクトル空間アクセス構造である。

証明 3.2

位数 2 の 2 次元ベクトル空間 $(Z_2)^2$ を考える。このとき、星アクセス構造 $\Gamma\langle S(P_0)\rangle = \{A_1, \cdots, A_r\}$ に対応する星グラフの頂点は、2 つの部分 $\{P_0\}$ および $\{P_1, \cdots, P_n\}$ に分割できる。参加者 P_0 にはベクトル $\phi(P_0) = (1,1)$ を、残りの参加者 P_i $(1 \le i \le n)$ にはベクトル $\phi(P_i) = (0,1)$ を与えたとする。つまり、同じ部分に含まれる参加者には同じベクトルを与える。このとき、

$$\phi(D) = (1,0) \in \langle \phi(P_i) : P_i \in A_j \subset P,\ 1 \le i \le n, 1 \le j \le r \rangle \ \Leftrightarrow\ B \in \Gamma$$

を確かめるのは容易である。同様に、位数 p の d 次元ベクトル空間において適当なベクトルを与えるときについても確かめることができる。ゆえに、星グラフに関するアクセス構造 $\Gamma\langle S(P_0)\rangle$ は、ベクトル空間アクセス構造である。

□

3.3　ファノ平面に関するアクセス構造

ファノ平面とは、位数 2 の有限射影平面であり、ファノ平面に関するアクセス構造を Γ_2 で表す(図 3.3 参照)。Γ_2 は会合数 1 を持ち、ランク（最小アクセス集合の参加者の最大人数）とコランク(最小アクセス集合の参加者の最小人数)共に 3 である。

補題 3.3

Γ_2 をファノ平面に関するアクセス構造であるとする。つまり、$\{P_1, P_2, P_3\}$, $\{P_1, P_4, P_7\}$, $\{P_1, P_5, P_6\}$, $\{P_2, P_4, P_6\}$, $\{P_2, P_5, P_7\}$, $\{P_3, P_4, P_5\}$, $\{P_3, P_6, P_7\}$ を基に持つ、7 人の参加者集合 $P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$ から成るアクセス構造である。このとき、アクセス構造 Γ_2 はベクトル空間アクセス構造である。

証明 3.3

位数 2 の 4 次元ベクトル空間 $(Z_2)^4$ を考える。$\phi : P \cup \{D\} \to (Z_2)^4$ を

$$\phi(D) = (1,0,0,0),\ \phi(P_1) = (1,0,1,0),\ \phi(P_2) = (0,1,1,0),\ \phi(P_3) = (0,1,0,0),$$
$$\phi(P_4) = (1,1,1,1),\ \phi(P_5) = (0,0,1,1),\ \phi(P_6) = (0,0,0,1),\ \phi(P_7) = (1,1,0,1)$$

によって定義される写像であるとする。ベクトル $\phi(D)$ が集合 $\{\phi(P_i) : P_i \in A\}$ のベクトルの線型結合である場合に限り、$A \subset \Pi$ ならば $A \in \Gamma_2$ であることを調べるのは難しくない。同様に、位数 p の d 次元ベクトル空間において適当なベクトルを与えるときについても確かめることができる。ゆえに、Γ_2 はベクトル空間 $(Z_2)^4$ 上のベクトル空間アクセス構造である。　□

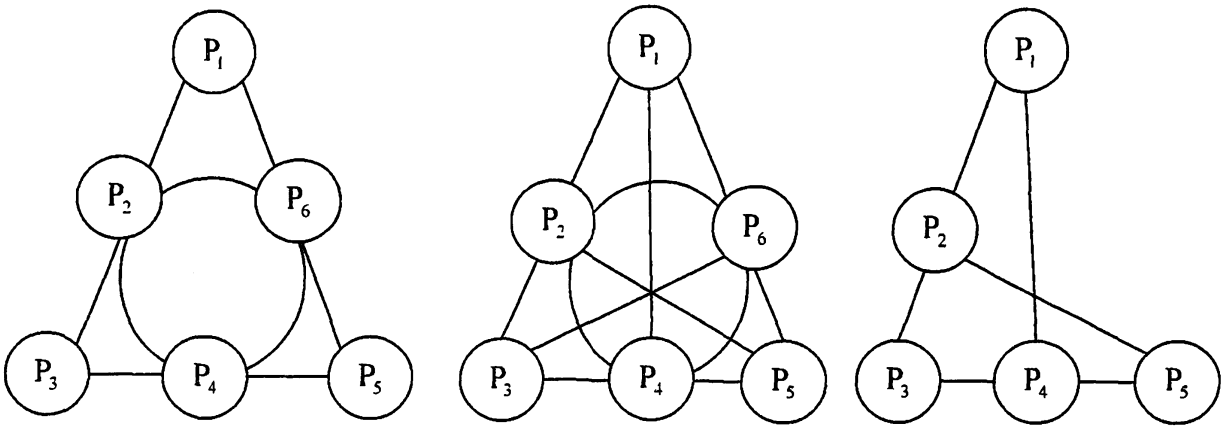
3.4 Γ_2に関連した3つのアクセス構造

前節までに、ファノ平面に関するアクセス構造Γ_2について紹介してきた。本節では、これに関連したアクセス構造を3つ：$\Gamma_{2,1}, \Gamma_{2,2}, \Gamma_{2,3}$ 紹介する(図3.4参照)。これらは会合数1である。以下に、各々の定義を示す。

定義3.1 Γ_2に関連したアクセス構造$\Gamma_{2,1}, \Gamma_{2,2}, \Gamma_{2,3}$

ファノ平面に関するアクセス構造Γ_2の参加者$P'=\{P_1,\cdots,P_7\}$の部分集合を$Q'=\{P_1,P_2,P_3,P_4,P_5,P_6\}$, $Q''=\{P_1,P_2,P_3,P_4,P_5\}$とする。このとき、アクセス集合$\Gamma_{2,1}, \Gamma_{2,2}$は部分集合$Q'$から、アクセス集合$\Gamma_{2,3}$は部分集合$Q''$から成る、以下の基を持つ族と定義する。

1) $\Gamma_{2,1} := \{\{P_1,P_2,P_3\}, \{P_1,P_5,P_6\}, \{P_2,P_4,P_6\}, \{P_3,P_4,P_5\}\}$
2) $\Gamma_{2,2} := \{\{P_1,P_2,P_3\}, \{P_1,P_5,P_6\}, \{P_2,P_4,P_6\}, \{P_3,P_4,P_5\}, \{P_1,P_4\}, \{P_2,P_5\}, \{P_3,P_6\}\}$
3) $\Gamma_{2,3} := \{\{P_1,P_2,P_3\}, \{P_3,P_4,P_5\}, \{P_1,P_4\}, \{P_2,P_5\}\}$



$\Gamma_{2,1}$ $\Gamma_{2,2}$ $\Gamma_{2,3}$

図3.4 Γ_2に関する3つのアクセス構造

参加者集合Π上のアクセス構造をΓとする。任意の部分集合$Q \subset P$ に関して、アクセス構造 Γ による部分集合Q 上の誘導構造は、$\Gamma(Q)=\{A \in \Gamma : A \subset Q\}$で定義される。つまり、アクセス構造$\Gamma_{2,1}$は、アクセス構造$\Gamma_2$による参加者部分集合$Q'$上の誘導構造$\Gamma_2(Q')=\{A' \in \Gamma_2 : A' \subset Q'\}$である。また、アクセス構造$\Gamma_{2,3}$は、アクセス構造$\Gamma_{2,2}$による参加者部分集合$Q''$上の誘導構造$\Gamma_{2,2}(Q'')$である。また、アクセス構造$\Gamma$の双対構造は、$\Gamma^* = \{A \subset P : P \setminus A \notin \Gamma\}$で定義される。つまり、

アクセス構造$\Gamma_{2,2}$は、$\Gamma_{2,1}$の双対構造$(\Gamma_{2,1})^* = \{A'' \subset Q' : Q' \setminus A'' \notin \Gamma_{2,1}\}$である。

補題 3.4

Γ_2に関連した3つのアクセス構造$\Gamma_{2,1}, \Gamma_{2,2}, \Gamma_{2,3}$は、ベクトル空間アクセス構造である。

証明 3.4

アクセス構造Γがベクトル空間アクセス構造ならば、その部分集合である誘導構造$\Gamma(Q)$もベクトル空間アクセス構造であることは明らかである。よって、$\Gamma_{2,1} = \Gamma_2(\{P_1, P_2, P_3, P_4, P_5, P_6\})$を確かめればよい。この結果から双対構造$(\Gamma_{2,1})^* = \Gamma_{2,2}$を確かめられ、さらに、$\Gamma_{2,3} = \Gamma_{2,2}(\{P_1, P_2, P_3, P_4, P_5\})$を調べることで補題3.4の結果を得る。 □

3.5 グラフに関するアクセス構造とベクトル空間アクセス構造との関係

会合数 1 のアクセス構造に関し、ベクトル空間アクセス構造とあるグラフによって与えられるアクセス構造は同値であるという次の定理が、Farre らによって与えられた。

定理 3.1

会合数1の参加者集合Π上のアクセス構造Γと以下の条件は同値：

1) Γ はベクトル空間アクセス構造である。
2) Γ は以下の構造のいずれかである。
   完全多部グラフに関するアクセス構造$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$
   星アクセス構造$\Gamma\langle S(P_0)\rangle$
   ファノ平面に関するアクセス構造 Γ_2
   Γ_2に関連したアクセス構造$\Gamma_{2,1}, \Gamma_{2,2}, \Gamma_{2,3}$

定理3.1の2)が1)の十分条件であることは、補題3.1, 3.2, 3.3, 3.4から明らかである。いま、1)が2)の必要条件であることについて確かめる。

Γ を、会合数1、corank$(\Gamma) \geqq 3$、基 Γ_0を持つ参加者集合Π上のベクトル空間アクセス構造であると仮定する。まず、$A_1, A_2, A_3 \in \Gamma_0$を、

$$A_1 \cap A_2 \neq \emptyset,\ A_1 \cap A_3 \neq \emptyset,\ A_2 \cap A_3 \neq \emptyset,\ A_1 \cap A_2 \cap A_3 \neq \emptyset$$

であるような、3つの異なる最小アクセス集合とすると、

$$(A_1 \cup A_2 \cup A_3) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_3) \cup (A_2 \cap A_3)) \in \Gamma$$

である。更に、$i=1,2,3$に関して$|A_i|=3$であり、$A_2 \cap A_3 \neq \varnothing$でもある。これより、会合数1、corank$(\Gamma) \geqq 3$である参加者集合$\Pi$上のベクトル空間アクセス構造$\Gamma$は、星アクセス構造$\Gamma\langle S(P_0)\rangle$、ファノ平面に関するアクセス構造 Γ_2、またはアクセス構造 $\Gamma_{2,1}$である。

次に、$|A_1| \geq 3$かつ$|A_2|=2$であるような任意の二つの最小アクセス集合に関し、$A_1 \cap A_2 \neq \varnothing$とすれば、

$$(A_1 \cup A_2) \cap (A \notin \Gamma$$

である。$|A_1| \geq 3$, $|A_2|=2$, $|A_3| \geq 2$であるような三つの異なる最小アクセス集合に関し、$\varnothing \neq A_1 \cap A_2 \neq A_2 \cap A_3 \neq \varnothing$とすると、

$$|A_1|=3,\ |A_3|=3,\ A_1 \cap A_3 \neq \varnothing,\ (A_1 \cup A_3) \setminus (A_2 \cup (A_1 \cap A_3)) \in \Gamma$$

となる。また、$\varnothing \neq A_1 \cap A_2 \neq A_1 \cap A_3 \neq \varnothing$とすれば、

$$|A_1|=3,\ A_2 \cap A_3 = \varnothing,\ (A_1 \cup A_2 \cup A_3) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_3)) \in \Gamma$$

となる。これより、会合数1、corank$(\Gamma)=2$を持つ、参加者集合Π上のベクトル空間アクセス構造 Γ は、完全多部分グラフ$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$、星アクセス構造$\Gamma\langle S(P_0)\rangle$、アクセス構造 $\Gamma_{2,2}$、またはアクセス構造 $\Gamma_{2,3}$である。

以上より、会合数1のベクトル空間アクセス構造Γは、完全多部グラフに関するアクセス構造$\Gamma\langle K_{m_1,\cdots,m_k}\rangle$、星アクセス構造$\Gamma\langle S(P_0)\rangle$、ファノ平面に関するアクセス構造 Γ_2、Γ_2に関連したアクセス構造$\Gamma_{2,1}, \Gamma_{2,2}, \Gamma_{2,3}$のいずれかであることが示せた。よって定理3.1の1)と2)は確かに同値である。

4. 終わりに

本稿ではShamirの(t, n)しきい値法をより一般的な状況としたアクセス構造を扱った。アクセス構造は、Brickellによってベクトル空間アクセス構造が考案されている。なかでも会合数1を持つ、グラフを用いたベクトル空間アクセス構造について紹介をしてきた。

一般にこれらの秘密分散の効率を測るパラメータとして、情報比 ρ が用いられる。Σは秘密情報の集合、ς_PはユーザーPが受け取る可能性のある分散情報の集合を意味する。情報比は、

$$\rho = \log|\Sigma| \ / \max_{P \in \Pi} \log|\varsigma_P|$$

で表され、すなわち秘密情報の長さと参加者に与えうる分散情報の最大長の長さの比を意味する。特に、アクセス構造Γを実現する完全な秘密分散法の最大の情報比を$\rho^*(\Gamma)$と表記し、最適情報比という。

ここで、情報比に関し、PadroとSaezによって一般化が与えられた独立シー

ケンス法について紹介をする。Γ を参加者集合Π上のアクセス構造であるとしよう。$\varnothing \neq B_1 \subset \cdots \subset B_m \notin \Gamma$を、$R \subset P$ によって独立に生成されるΠの部分集合の数列とする。すなわち、$i=1,\cdots,m$であるとき、B_0が空集合であり$B_i \cap X_i \in \Gamma$かつ$B_{i-1} \cap X_i \notin \Gamma$であるような$X_1,\cdots,X_m \subset R$が存在する。このとき、$R \in \Gamma$ならば$\rho^*(\Gamma) \leq |R|/(m+1)$であり、$A \notin \Gamma$ならば$\rho^*(\Gamma) \leq |R|/m$となることが知られている。このシーケンス法を用いると、定理3.1が$\rho^*(\Gamma) > 2/3$と同値であることがいえる。この詳細な考察については、参考文献[2]の第3節に詳しい。

参考文献

[1] E. F. Brickell : Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 6 (1989), pp. 105 - 113.

[2] J. M. Farre, C. Padro : Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics*, 154 (2006), pp. 552 - 563

[3] A. Shamir : How to share a secret. *Communications of the ACM*, 22 (1979), pp. 612 - 613.